

# TOOLS FOR WEBSERVER FOOT PRINTING

In Kali : 1.Netcat

2.Telnet

3.Uniscan

4.Nmap

5.Skipfish

In Windows: 1.Httppercon

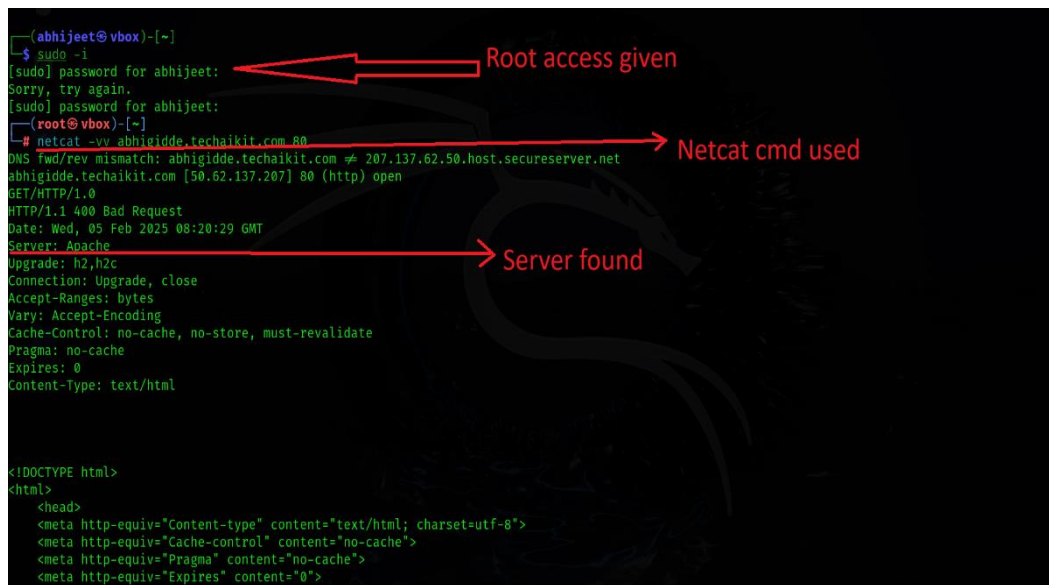
2.Idserver

Online : 1.Netcraft

In Kali :

**1.NETCAT** : shows the server on which the website is running

- netcat -vv targetip/domain 80



```
(abhiijeet@ vbox) - [~]
$ sudo -i
[sudo] password for abhiijeet:
Sorry, try again.
[sudo] password for abhiijeet:
(root@ vbox) - [~]
# netcat -vv abhigidde.technaikit.com 80
DNS fwd/rev mismatch: abhigidde.technaikit.com < 207.137.62.50.host.secureserver.net
abhigidde.technaikit.com [50.62.137.207] 80 (http) open
GET/HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Wed, 05 Feb 2025 08:20:29 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, close
Accept-Ranges: bytes
Vary: Accept-Encoding
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
    <meta http-equiv="Cache-control" content="no-cache">
    <meta http-equiv="Pragma" content="no-cache">
    <meta http-equiv="Expires" content="0">
```

## 2. TELNET : shows the server of the website

- telnet targetip/domain 80

```
sent 13, rcvd 10402
[root@vbox]~# telnet abhigiddde.techaikit.com 80
Trying 50.62.137.207...
Connected to abhigiddde.techaikit.com.
Escape character is '^]'.
GET/HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Wed, 05 Feb 2025 08:28:53 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, close
Accept-Ranges: bytes
Vary: Accept-Encoding
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-type" content="text/html; charset=utf-8">
<meta http-equiv="Cache-control" content="no-cache">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Expires" content="0">
<meta name="Viewport" content="width=device-width, initial-scale=1.0">
<title>400 Bad Request</title>
```

telnet cmd used

get method used for info exchange

server details found

other details of the target / domain

## 3. UNISCAN :

- uniscan -u targetip/domain -g

This gives specific info about the domain / website

```
</footer>
</body>
</html>
Connection closed by foreign host.

[root@vbox]~# uniscan -u abhigiddde.techaikit.com -g
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3

Scan date: 5-2-2025 14:1:59

| Domain: http://abhigiddde.techaikit.com/
| Server: Apache
| IP: 50.62.137.207

| Looking for Drupal plugins/modules
| GET,POST,OPTIONS,HEAD

Can't locate object method "get_connections" via package "1" (perhaps you forgot to load "1"? at /usr/share/perl5/LWP/UserAgent.pm line 890.

[root@vbox]~#
```

uniscan cmd with -g

server details

- uniscan -u targetip/domain -j

This gives all the details related to the domain

```
(root@vbox)-[~]
# uniscan -u abhigidde.techaikit.com -j
#####
# Uniscan project
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 5-2-2025 14:3:51

Domain: http://abhigidde.techaikit.com/
Server: Apache
IP: 50.62.137.207

PING
PING abhigidde.techaikit.com (50.62.137.207) 56(84) bytes of data.
64 bytes from 207.137.62.50.host.secureserver.net (50.62.137.207): icmp_seq=1 ttl=42 time=283 ms
64 bytes from 207.137.62.50.host.secureserver.net (50.62.137.207): icmp_seq=2 ttl=42 time=259 ms
64 bytes from 207.137.62.50.host.secureserver.net (50.62.137.207): icmp_seq=3 ttl=42 time=491 ms
64 bytes from 207.137.62.50.host.secureserver.net (50.62.137.207): icmp_seq=4 ttl=42 time=249 ms

--- abhigidde.techaikit.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 248.524/320.509/491.148/99.321 ms
```

uniscan cmd with -j

server details found

as -j is used gives all the details of target

#### 4.NMAP :

- `nmap -sV --script=http-trace -p80 targetip/domain`

This tells whether the domain is affected with the trace vulnerability or not.

If yes we can hijack the session

```
(root@vbox)-[~]
# nmap -sV --script=http-trace -p80 abhigidde.techaikit.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 14:07 IST
Nmap scan report for abhigidde.techaikit.com (50.62.137.207)
Host is up (0.32s latency).
rDNS record for 50.62.137.207: 207.137.62.50.host.secureserver.net

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.83 seconds

(root@vbox)-[~]
#
```

nmap trace is used to know that trace vulnerability is present on server or not

if trace vulnerability is present server shows enabled option else nothing

- `nmap -sV --script=http-userdir-enum targetip/domain`

This gives username of user and any input it gives to the website

```
(root@vbox)-[~]
# nmap -script=http-userdir-enum abhigidde.techaikit.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 14:12 IST
Nmap scan report for abhigidde.techaikit.com (50.62.137.207)
Host is up (0.26s latency).
rDNS record for 50.62.137.207: 207.137.62.50.host.secureserver.net
Not shown: 974 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
70/tcp    open  gopher
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
990/tcp   closed ftps
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp   open  mysql
8443/tcp   closed https-alt
50000/tcp  closed ibm-db2
50001/tcp  closed unknown
50002/tcp  closed iiimsf
50003/tcp  closed unknown
50006/tcp  closed unknown
50300/tcp  closed unknown
50389/tcp  closed unknown
50500/tcp  closed unknown
50636/tcp  closed unknown
```

userdir-enum is used for any input from the user to the server

if there is any input such as username , adminlogin , email is shown here , but if not then it shows none

- nmap -script=http-waf-detect targetip/domain

Informs that firewall or ids is present or not for domain.

```
(root@vbox)-[~]
# nmap -script=http-waf-detect abhigidde.techaikit.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 14:12 IST
Nmap scan report for abhigidde.techaikit.com (50.62.137.207)
Host is up (0.32s latency).
rDNS record for 50.62.137.207: 207.137.62.50.host.secureserver.net
Not shown: 974 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
70/tcp    open  gopher
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
990/tcp   closed ftps
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp   open  mysql
8443/tcp   closed https-alt
50000/tcp  closed ibm-db2
50001/tcp  closed unknown
50002/tcp  closed iiimsf
50003/tcp  closed unknown
50006/tcp  closed unknown
50300/tcp  closed unknown
50389/tcp  closed unknown
50500/tcp  closed unknown
50636/tcp  closed unknown
```

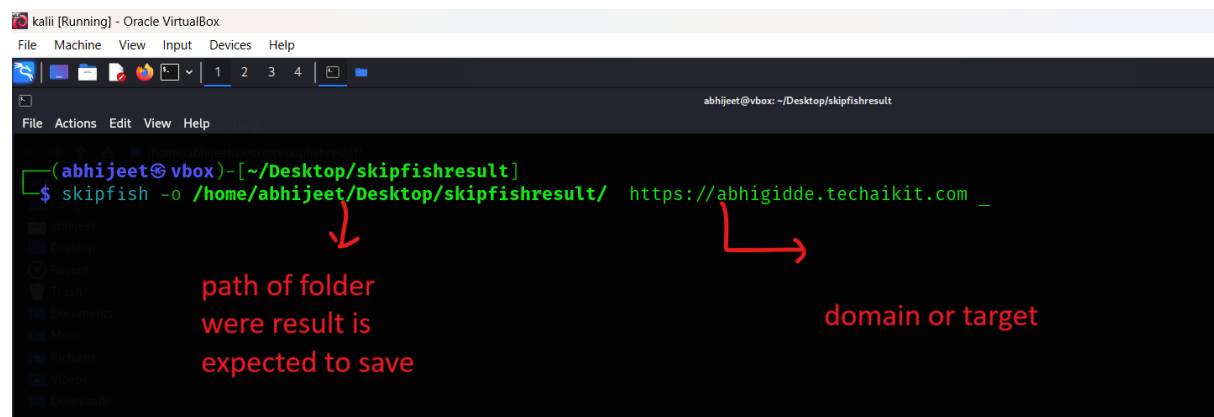
used to check firewall or ids is present or not

## 5.SKIPFISH

Gives complete information such as imgs , videos and all content used in the website .

The data is stored in folder .

Command of skipfish :



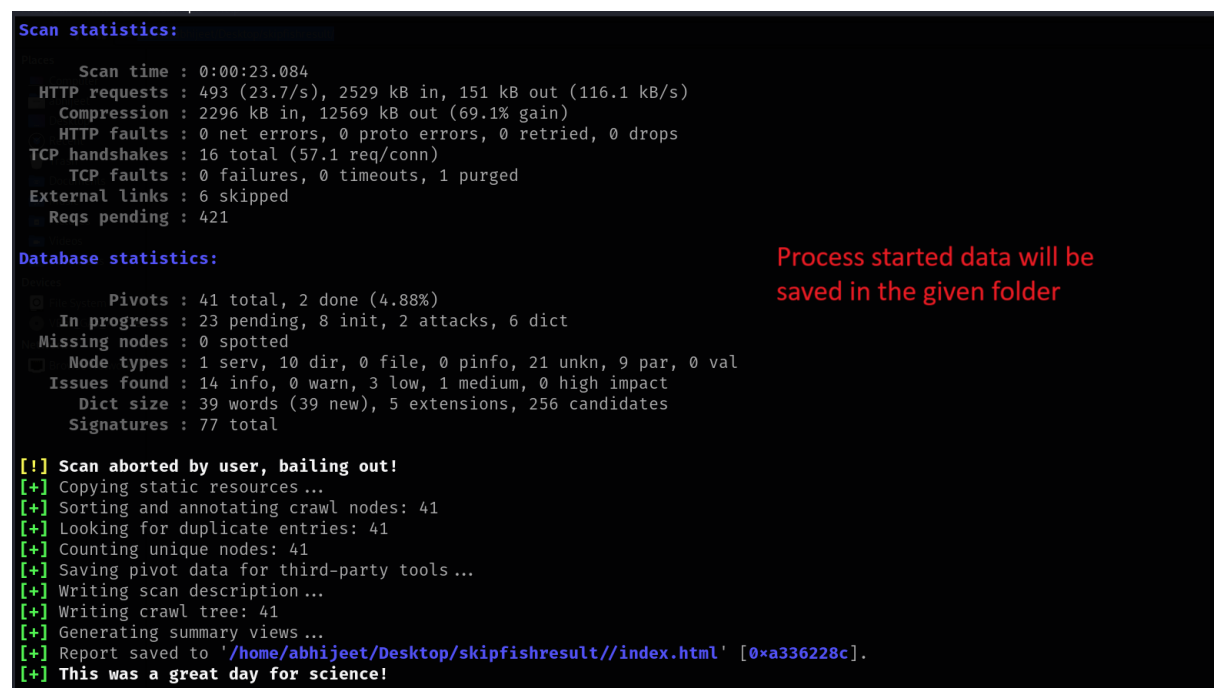
```
kalii [Running] - Oracle VirtualBox
File Machine View Input Devices Help
abhiijeet@vbox: ~/Desktop/skipfishresult
File Actions Edit View Help

(abhiijeet@vbox)-[~/Desktop/skipfishresult]
$ skipfish -o /home/abhiijeet/Desktop/skipfishresult/ https://abhigidde.techaikit.com _
```

path of folder  
were result is  
expected to save

domain or target

Process :



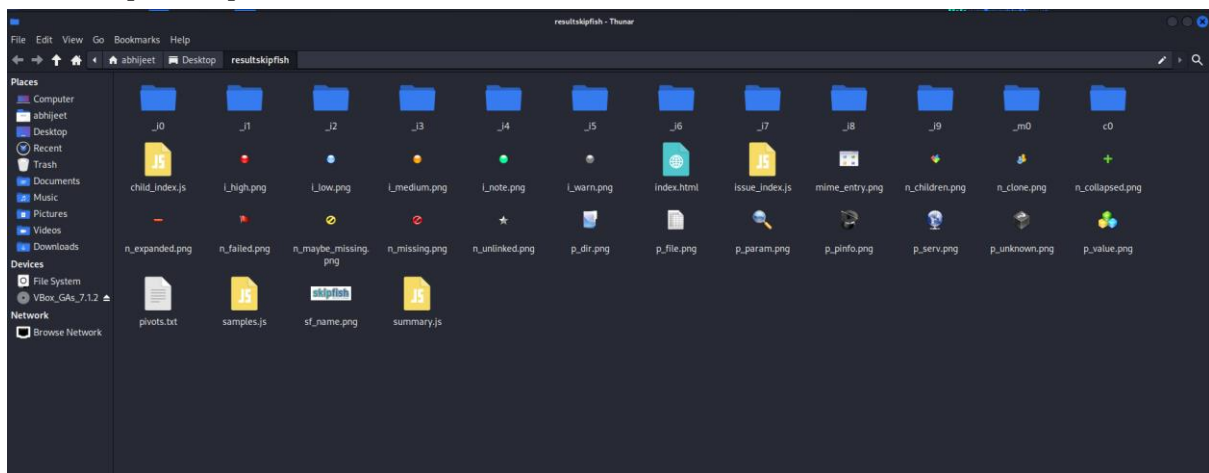
```
Scan statistics:
  Scan time : 0:00:23.084
  HTTP requests : 493 (23.7/s), 2529 kB in, 151 kB out (116.1 kB/s)
  Compression : 2296 kB in, 12569 kB out (69.1% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 16 total (57.1 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 6 skipped
  Reqs pending : 421

Database statistics:
  Pivots : 41 total, 2 done (4.88%)
  In progress : 23 pending, 8 init, 2 attacks, 6 dict
  Missing nodes : 0 spotted
  Node types : 1 serv, 10 dir, 0 file, 0 pinfo, 21 unkn, 9 par, 0 val
  Issues found : 14 info, 0 warn, 3 low, 1 medium, 0 high impact
  Dict size : 39 words (39 new), 5 extensions, 256 candidates
  Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 41
[+] Looking for duplicate entries: 41
[+] Counting unique nodes: 41
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 41
[+] Generating summary views ...
[+] Report saved to '/home/abhiijeet/Desktop/skipfishresult//index.html' [0xa336228c].
[+] This was a great day for science!
```

Process started data will be  
saved in the given folder

Result [DATA] saved in folder :



## In Windows:

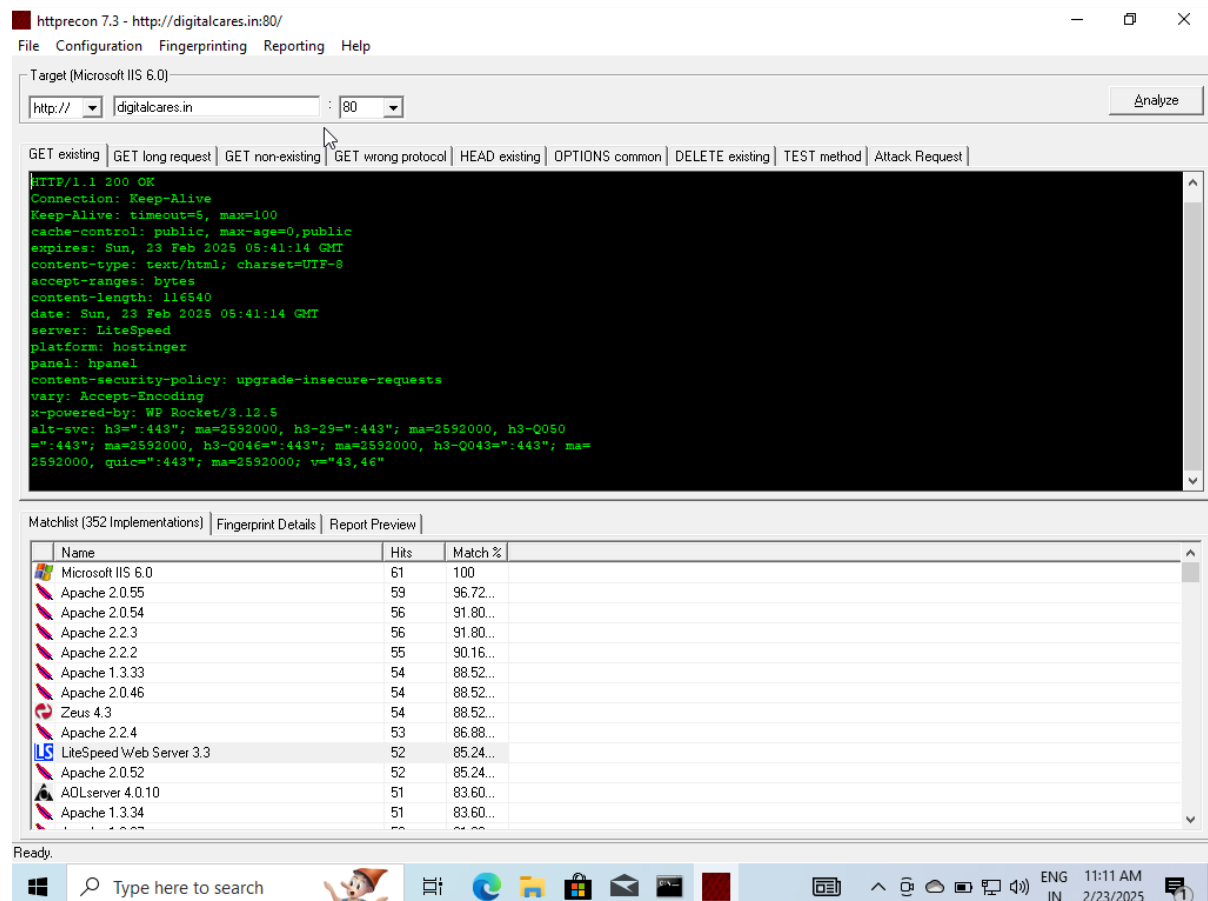
**1.Idserver :** Application installed in windows through <https://www.grc.com>.

It takes the ip address or the domain name and gives the server and relevant information related to domain.



## 2.Httprecon:Application installed in windows through <https://www.computec.ch> .

This also gives the relevant information about the server of the entered ip address or domain but gives specific details of the server like the current version of the server in use.




**Online : Netcraft :** This is a online tool for web server footprinting. This gives a very detailed information about the domain .

This is shown below:

- 1.Entering the domain
2. Detailed output report of the scanned website



# 1.Entering the domain


[LEARN MORE](#)[REPORT FRAUD](#)

## What's that site running?


Find out the infrastructure and technologies used by any site using results from our **internet data mining**

Example: <https://www.netcraft.com>

LOOK UP



# 2.Output:

[LEARN MORE](#)[REPORT FRAUD](#)

## Site report for https://digitalcares.in

🔍 Look up another site?

Share: [🌐](#) [X](#) [f](#) [in](#) [v](#)

### Background

Site title	DigitalCares   Mob App   Web Designing   Seo   Digital Marketing	Date first seen	July 2020
Site rank	Not Present	Primary language	Unknown
Description	Digital Cares is a Mobile App Development   Web Designing   SEO   Digital Marketing & Advertising Agency offering it services across India.		

### Network

Site	<a href="https://digitalcares.in">https://digitalcares.in</a>	Domain	<a href="https://digitalcares.in">digitalcares.in</a>
Netblock Owner	unknown	Nameserver	ns1.dns-parking.com
Hosting company	Hostinger Group	Domain registrar	registry.in



Network

Site	<a href="https://digitalcares.in">https://digitalcares.in</a>	Domain	<a href="https://digitalcares.in">digitalcares.in</a>
Netblock Owner	unknown	Nameserver	ns1.dns-parking.com
Hosting company	Hostinger Group	Domain registrar	registry.in
Hosting country	IN	Nameserver organisation	whois.hostinger.com
IPv4 address	82.180.142.41 <a href="#">(VirusTotal)</a>	Organisation	Editoriall, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	<a href="#">AS47583</a>	DNS admin	dns@hostinger.com
IPv6 address	2a02:4780:11:975:0:914:59d2:2	Top Level Domain	India (.in)
IPv6 autonomous systems	<a href="#">AS47583</a>	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

IP delegation

IPv4 address (82.180.142.41)

IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 82.0.0.0-82.255.255.255	Netherlands	82-RIPE	RIPE Network Coordination Centre
↳ 82.180.128.0-82.180.191.255	Germany	DE-TERRATRANSIT-20031009	TerraTransit AG
↳ 82.180.136.0-82.180.143.255	United States	HOSTINGER-HOSTING	
↳ 82.180.140.0-82.180.143.255	India	HOSTINGER-HOSTING	
↳ 82.180.142.41	India	HOSTINGER-HOSTING	



↳ 2a02:4780:11:975:0:914:59d2:2

India

HOSTINGER-HOSTING

HOSTINGER IN

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

